

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

SUSAN CLEMENTS-JEFFREY, et al., :

 Plaintiffs, :

 vs. :

CITY OF SPRINGFIELD, OHIO, et al., :

 :

 Defendants

Case No. 3:09-cv-84
JUDGE WALTER HERBERT RICE

DECISION AND ENTRY SUSTAINING PLAINTIFF'S MOTION IN LIMINE TO
EXCLUDE TESTIMONY OF DR. ARTHUR J. JIPSON (DOC. #93)

Plaintiffs have moved the Court for an Order prohibiting Defendants from introducing, at trial, the testimony of Defendants' expert witness, Dr. Arthur J. Jipson, an Associate Professor of Sociology and Director of the Criminal Justice Studies Program at the University of Dayton. For the reasons stated below, the Court sustains Plaintiffs' motion (Doc. #93).¹

¹ Defendants argue that Plaintiffs' motion is not yet ripe because the Court has not yet ruled on Defendants' motions for summary judgment. A separate Decision and Entry ruling on those motions, however, will be issued within a few days, and counsel have already been orally advised as to the Court's ruling therein.

I. Dr. Jipson's Proposed Testimony

Defendants offer Dr. Jipson as a "contextual expert," who can help to explain the problems of laptop computer theft, the need for theft recovery tools, and how those tools operate. He also intends to offer his expert opinion that Plaintiffs had no reasonable expectation of privacy in communications via the Internet.

Dr. Jipson offers five conclusions in his expert report:

1. It is not reasonable to believe that electronic communication is private online.
2. Only the original owner of a computer can have meaningful knowledge of security protection it contains. Any subsequent user of a laptop cannot assume automatic protection of any kind.
3. Computer, laptop, and electronic equipment theft is a serious social and criminological problem for organizations, businesses and individuals that requires reasonable remote and location-specific security solutions.
4. When a company activates system operation software capture for security reasons, the representatives of the company/ employees cannot predict the nature of the material that will be accessed.
5. Security and theft protection tools are necessary and proper tools to combat computer theft.

Ex. 1 to Jipson Decl. attached to Absolute Defs.' Mot. for Summ. J.

II. Federal Rule of Evidence 702

Plaintiffs maintain that Dr. Jipson's testimony does not satisfy the standards for expert witness testimony under Federal Rule of Evidence 702. That Rule states:

If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case.

Fed. R. Evid. 702.

In *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993), the Supreme Court held that the trial judge must perform a "gatekeeping" function with respect to expert witness testimony. *Id.* at 596. The court must ensure that expert witness testimony "is not only relevant, but reliable." *Id.* at 589.

With respect to relevance, the question is whether the expert testimony being proffered "is sufficiently tied to the facts of the case that it will aid the jury in resolving a factual dispute." *Id.* at 591 (quoting *United States v. Downing*, 753 F.2d 1224, 1242 (3d Cir. 1985)). With respect to the question of reliability, where the expert's testimony is based on something other than scientific knowledge, the court is given "broad latitude" in determining whether the proffered testimony is sufficiently reliable. *See Kumho Tire Co., Ltd. v. Carmichael*, 526 U.S. 137, 141-42 (1999).

III. Qualifications

The Court turns first to the question of Dr. Jipson's qualifications. The parties disagree on whether Dr. Jipson is qualified, by virtue of his "knowledge, skill, experience, training, or education," to offer expert witness testimony on the topics of Internet privacy, laptop computer theft, and theft recovery tools. See Fed. R. Evid. 702.

Defendants note that Dr. Jipson has taught classes in sociology and criminology at the university level for almost 20 years. He teaches classes on cyber crime and Internet deviance. Internet crime and privacy issues have been a consistent area of interest for him. He teaches a course on Internet and Popular Culture, which includes a section on Internet privacy. He has also written numerous articles that touch on these topics. Plaintiffs note, however, that none of these articles deals exclusively with the subject of his opinions in this case, and that he has never testified as an expert witness on this topic. Jipson Dep. at 10-12, 33-34, 48, 56-58, 62.

The Court need not decide whether Dr. Jipson possesses the requisite qualifications to offer the proposed expert witness testimony. Assuming *arguendo* that he is qualified, his testimony is nevertheless inadmissible for other reasons.

IV. Whether Plaintiffs Had a Reasonable Expectation of Privacy Is a Question of Law and, Given that Dr. Jipson's Opinion Is Contrary to Law, His Opinion on this Subject is Not Relevant to the Issues in this Case.

Based on his knowledge, education, and experience, Dr. Jipson first offers

his expert opinion that no one, including Plaintiffs, has a reasonable expectation of privacy in Internet communications. As will be noted in the Decision and Entry ruling on Defendants' motions for summary judgment, this is a threshold issue in this case, and a necessary prerequisite for each of Plaintiffs' claims. *See United States v. Jones*, 75 F. App'x 398, 400 (6th Cir. 2003) (noting that a reasonable expectation of privacy is "tantamount to 'standing' in other contexts").

The question of whether Plaintiffs had a reasonable expectation of privacy in their Internet communications, however, is a question of law to be decided by the Court. *See id.*; *United States v. Welliver*, 976 F.2d 1148, 1151 (8th Cir. 1992). This renders Dr. Jipson's "opinion" on this topic absolutely irrelevant. What makes his "opinion" even more troublesome is that it is contrary to case law.

Numerous courts have recognized that individuals have an objectively reasonable expectation of privacy in their personal computers. *See United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007) (holding that the defendant "had a legitimate, objectively reasonable expectation of privacy in his personal computer"); *United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) ("Individuals generally possess a reasonable expectation of privacy in their home computers."); *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001) ("Home owners would of course have a reasonable expectation of privacy in their homes and in their belongings - including computers - inside the home.").

Personal computers that are password-protected are subject to even greater privacy protection. *See United States v. Aaron*, 33 F. App'x 180 (6th Cir. 2002) (in assessing the scope of a privacy interest, the court should examine "whether the relevant files were password-protected or whether the defendant otherwise manifested an intention to restrict third-party access."); *United States v. Lucas*, 640 F.3d 168 (6th Cir. 2011) (holding that the district court did not err in holding that the search of a laptop computer that was not password-protected was akin to the search of a closed, unlocked container); *United States v. Buckner*, 473 F.3d 551, 554 n.2 (4th Cir. 2007) (district court's finding that defendant had a reasonable expectation of privacy in password-protected files was not clearly erroneous).

As to electronic communications sent over the Internet, the Sixth Circuit has recently held that "a subscriber enjoys a reasonable expectation of privacy in the contents of emails 'that are stored with, or sent or received through, a commercial [Internet service provider].'" *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010), *reh'g and reh'g en banc denied* (2011) (quoting *Warshak v. United States*, 490 F.3d 455, 473 (6th Cir. 2007)). The court found that "the very fact that information is being passed through a communications network is a paramount Fourth Amendment consideration." *Id.* at 285. It also stated that "the Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish." *Id.* The Sixth Circuit noted that Fourth

Amendment protects traditional forms of communications such as telephone calls and letters, and found that “it would defy common sense to afford emails lesser Fourth Amendment protection.” *Id.* at 286.

The court in *Warshak* also held that even though email had to pass through an Internet service provider (“ISP”), and even though that provider may have contractually reserved the right to access the subscriber’s email in certain circumstances, neither the ability of the ISP to gain that access, nor its contractual right to do so, extinguished the user’s reasonable expectation of privacy. *Id.* at 286-87.

In a similar vein, the Supreme Court recently assumed, without deciding, that a city employee had a reasonable expectation of privacy in text messages sent and received on a pager provided by his employer. *See City of Ontario v. Quon*, 130 S. Ct. 2619, 2630 (2010).

These holdings can logically be extended to cover instant messages and webcam communications, the types of electronic communications at issue in this case. Applicable statutes also shed light on whether an individual has an objectively reasonable expectation of privacy in electronic communications. The Stored Communications Act (“SCA”), 18 U.S.C. § 1701 *et seq.*, at issue in *Warshak* and *Quon* and the subject of one of Plaintiffs’ claims in this case, specifically prohibits the intentional, unauthorized access of stored communications such as email. The Electronic Communications Privacy Act (“ECPA”), 18 U.S.C. §

2511, also the subject of one of Plaintiffs' claims in this case, specifically prohibits the intentional, unauthorized interception, disclosure, and use of wire, oral, and electronic communications.

Based on these statutes and on the above-cited case law, the Court concludes that Dr. Jipson's expert "opinion," that no one has an objectively reasonable expectation of privacy in password-protected Internet communications, is contrary to law, and thus not relevant to the issues in this litigation.

The Court finds it curious that despite Dr. Jipson's broadly stated expert opinion -- that there is no reasonable expectation of privacy in communications via the Internet -- Defendants did not argue this in their motions for summary judgment. Rather, they argued only that Plaintiffs lacked an objectively reasonable expectation of privacy because they knew or should have known that the laptop computer being used by Clements-Jeffrey was stolen.² The Court also finds it curious that, in formulating his opinion, Dr. Jipson did not consider this fact at all. Nor did he take the statutory prohibitions set forth in the ECPA and the SCA into account. Jipson Dep. at 81-82, 85-86, 135-36. As Plaintiffs note, Dr. Jipson completely ignored these "core issues."

In any event, the question of whether Plaintiffs had an objectively reasonable expectation of privacy in their Internet communications is a question of law to be

² As discussed in the Decision and Entry ruling on those motions for summary judgment, the question of whether Plaintiffs knew or should have known that the laptop was stolen is a factual dispute that must be resolved by a jury.

determined by the Court. This renders Dr. Jipson's opinion on this topic completely irrelevant, even more so in light of the fact that it is contrary to case law. For these reasons, the Court finds that his opinion on this topic is inadmissible.³

V. Even Though the Remainder of Dr. Jipson's Proposed Expert Witness Testimony May Assist the Jury In Understanding Some of the Evidence, It Is Excludable Under Federal Rule of Evidence 403.

Dr. Jipson also intends to offer expert witness testimony concerning the pervasive problem of laptop computer theft and the need for theft recovery tools. In addition, he intends to explain to the jury that theft recovery tools are often present on laptop computers, and when those theft recovery tools are activated, it is difficult to predict the nature of the material that will be accessed.⁴ Defendants argue that because these topics are beyond the actual knowledge and expertise of jurors, Dr. Jipson's testimony will assist the jury in its understanding of the relevant subject matter.

In addition to rendering an expert "opinion" on a topic, an expert witness may also be permitted to provide background information on a particular topic if it

³ Having found that Dr. Jipson's testimony on this topic is irrelevant, the Court need not address the question of whether it is reliable.

⁴ To the extent that Defendants seek to introduce this particular testimony to support their claim that Plaintiffs had no reasonable expectation of privacy in their Internet communications, it is irrelevant for the reasons previously discussed.

will assist the jury in understanding a particular issue. 4 Jack Weinstein & Margaret Berger, *Weinstein on Evidence* § 702.02[2] (2d ed. 2006); *United States v. Mulder*, 272 F.3d 91, 102 (2d Cir. 2001) (“The government is free to offer expert testimony both as background for an offense and to assist in proving one or more elements of the offense.”).

Even though expert witness testimony may be relevant and may assist the jury in understanding the issues, it is nevertheless subject to the balancing test set forth in Federal Rule of Evidence 403. Rule 403 provides that, “[a]lthough relevant, evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence.”

Plaintiffs maintain that whatever little probative value the remainder of Dr. Jipson’s testimony may have, it is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury. The Court agrees. In assessing the probative value of certain testimony, a court may consider what other evidentiary alternatives are available. If alternatives are readily available that have the same or greater probative value, but a lower danger of unfair prejudice or confusion of the issues, the court may exclude testimony on that basis. *See Old Chief v. United States*, 519 U.S. 172, 183-85 (1997).

In this case, the Court presumes that Defendant police officers Geoffrey Ashworth and Neil Lopez, and Absolute Software's theft recovery officer Kyle Magnus will be called to testify at trial. They will likely testify about the high number of laptop computers that are reported stolen, and about how theft recovery tools may be used to assist law enforcement officials in tracing stolen laptops.

Dr. Jipson testified that he was generally familiar with the operation of various theft recovery tools, including Absolute Software's "LoJack for Laptops," the theft recovery system that was used in this case. Jipson Dep. at 46. However, in the Court's view, Magnus and other Absolute Software employees are in a much better position to describe to a jury how the LoJack system works. They are also in a much better position to explain the various remote access tools used to trace the stolen laptop. In the Court's view, the testimony of these witnesses has significantly greater probative value than that of Dr. Jipson. The Court therefore concludes that the probative value of the remainder of Dr. Jipson's testimony is very slight.

Moreover, Magnus and other Absolute employees will undoubtedly testify about the prevalence of laptop computer theft, theft recovery tools in general, and about LoJack for Laptops in particular. They will also undoubtedly testify about how difficult it is to predict the nature of material that will be accessed when using certain theft recovery tools. Therefore, Dr. Jipson's testimony on these same topics would amount to "needless presentation of cumulative evidence."

In light of the opinions expressed in Dr. Jipson's expert report, there are also significant risks in allowing him to present "expert" testimony concerning these issues. Dr. Jipson believes that no one has any objectively reasonable expectation of privacy in Internet communications, an opinion the Court has found to be contrary to law, and thus inadmissible at trial. Given the likelihood that his belief would creep into his testimony on these other topics, there is a danger that the jury might be misled or confused.

Dr. Jipson is also of the opinion that theft recovery tools, presumably like those used in this case, are "necessary and proper" for combatting the problem of computer theft. Yet, in formulating his opinions, he admits that he completely failed to consider the statutory prohibitions set forth in the ECPA and SCA. This significantly increases the risk that the jury will be misled by his testimony. If the jury determines that Plaintiffs neither knew nor should have known that the laptop computer was stolen, the jury will then be called upon to determine whether the Absolute Defendants' efforts to recover the stolen laptop violated the ECPA or SCA, or otherwise invaded Plaintiffs' protected privacy interests. Dr. Jipson's opinions completely ignore these core issues.

Plaintiffs argue that a jury might give Dr. Jipson's "expert" witness testimony undue weight. They further argue that the admission of his testimony might invite jury nullification. Expert witness testimony that Plaintiffs' beliefs in privacy were unwarranted and that law enforcement should be given significant


leeway in recovering stolen laptops could invite the jury to find that the ends justified the means, regardless of whether Defendants' tactics violated the law or invaded Plaintiffs' privacy rights. In the Court's view, Plaintiffs' concerns are not unfounded.

The Court concludes that the slight probative value of Dr. Jipson's testimony on the remainder of the issues is substantially outweighed by the danger of confusion of the issues and misleading the jury. Quite simply, other witnesses are better equipped to provide the same "background" information to the jury, and can do so without the risks discussed above. Therefore, although relevant, Dr. Jipson's testimony on these topics is inadmissible under Federal Rule of Evidence 403.

VI. Conclusion

For the reasons set forth above, the Court SUSTAINS Plaintiffs' Motion in Limine to Exclude Testimony of Dr. Arthur J. Jipson (Doc. #93).

Date: July 27, 2011



WALTER HERBERT RICE
UNITED STATES DISTRICT JUDGE

Copies to:

Counsel of Record